Section III: **Application Security**
Title: **Systems Development Life Cycle (SDLC) Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **June 5, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To ensure that North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices include security within their Systems Development Life Cycle (SDLC) methodology.

STANDARD

1.0 Background

SDLC is a structured process developed to ensure that essential steps and activities are performed at appropriate times during system development. These processes lead to a cost effective use of resources and result in an information system that meets the needs of the project sponsor and stakeholders. Weaving security into the process will lead to the inclusion of security elements in the system development life cycle at the time when they can be most easily addressed.

2.0 System Development Life Cycle Security

2.1 Information System Development

Divisions and Offices shall address, at a minimum, the following information security issues while engaged in the information system development process:

- Evaluate the potential for compromise to other information systems in production
- Assess the impact to the confidentiality, integrity, and availability of the data stored on the information system
- Determine the threat of malicious code being inserted during information system coding

2.2 In-House vs. Third-Party Vendors

The five SDLC security phases listed in Section 2.3 apply to information systems that are built 'in-house" by Division or Office workforce members. Divisions and Offices must ensure that appropriate information system security measures are addressed for those information systems that are third-party vendor acquired. The same requirements shall also be included in any agreement where a third-party is contracted to build a new system. Divisions and Offices must comply with all contract laws, rules and policies when negotiating information system contracts with third-party vendors. ISO/IEC 27002:2005 Section 4.2.2 has a detailed listing of security requirements along with terms and conditions that must be considered for third-party vendor contracts.

2.3 Five SDLC Security Phases

All Divisions and Offices project plans that include information system development shall, at a minimum, include the following five phases:

- Phase I – Initiation Phase
- Phase II – Development Phase
- Phase III – Implementation Phase
- Phase IV – Operation and Maintenance Phase
- Phase V – Disposition Phase

3.0 Phase I - Security in the Initiation Phase

In the Initiation Phase, it is the responsibility of the Division or Office to ensure that development of the information system is justified. All reference materials used to justify the inception of an information system shall be documented, secured, and safeguarded. The following business requirements must be documented, analyzed, and included in the justification documentation:

- Synopsis of why business requirements can be met only with the proposed information system
- Explanation as to why the existing information systems cannot be updated to fulfill business needs
- Details about suitable packaged information system solutions investigated and why these packages will not meet the business requirements
- Documentation that the Division or Office has adequate resources to support the estimated project timeline
- Commitment that the Division and Office will support and maintain the information system during its required lifetime

The Divisions and Offices are to establish information security categories for all information systems in development. Assigned workforce members are responsible for completing the categorization process. The Divisions and Offices must adhere to the NC DHHS Security Standards, Application Security Standards – Information System Security Plan Standard when categorizing information system security. Once the categorization of security is complete, results shall be documented, secured, and safeguarded for auditing purposes.

Divisions and Offices must complete a risk assessment process in the Initiation Phase by adhering to the NC DHHS Security Standards, Administrative Security Standards – Information Security Risk Management Standard. The results of the risk assessment process shall be documented, secured, and safeguarded for auditing purposes.

4.0 Phase II - Security in the Development Phase

Divisions and Offices must ensure that information system development be performed based upon segregation of duties. Segregation of duties is an integral part of a successful information security program that reduces the risk of accidental and/or deliberate system compromise. Please see the NC DHHS Security Standards, Administrative Security Standards – Personnel Issues Related to Information Security Standard.

Test and Development environments shall be segregated and not accessible to Production or User Desktop networks.

Divisions and Offices must ensure that workforce members perform proper security functions in the Development Phase. Workforce members must properly perform the following functions:

A. Identify, document, secure, and safeguard the following risk assessment process attributes found in Section 3.0 Phase I – Security in the Initiation Phase:

   1. Identify information system vulnerabilities as well as threats to those vulnerabilities, and ensure that proper security is maintained during vulnerability management, Divisions and Offices management must adhere to the NC Statewide Information Security Manual, Version No. 1 – Chapter 4 – Purchasing and Maintaining Commercial Software, Section # 01: Purchasing and Installing Software – Standard 040106 – Technical Vulnerability Management.

   2. Determine the impact that loss of confidentiality, integrity, or availability of data and/or information would have on a Division or Office's operations (to include, but not limited to mission, functions, image, or reputation) if there were a threat exploitation of identified vulnerabilities.

   3. Identify and remediate any deficient information system management, operational and technical security controls.

B. Research and document applicable state and federal laws and regulations to assist in defining the necessary information system security requirements. The focus of the research and documentation should concentrate on, but not be limited to:

   1. Requirements to establish baseline criteria for information system confidentiality, integrity, and availability
   2. Once the research and documentation are complete, recorded results shall be secured and safeguarded

C. Develop and adhere to proper security assurance methods. Assurance methods must ensure that security controls being acquired will perform correctly and will have the desired effect in the Division and Office system production environment.

D. Analyze the costs associated with implementing security controls into the information system development. The cost information associated with system security controls must be found in the risk assessment process that was performed in Section 3.0, Phase I – Security in the Initiation Phase.

E. Prepare an Information System Security Plan to ensure required security controls are fully documented. Please see the NC DHHS Security Standards, Application Security Standards – Information System Security Plan Standard for further information regarding the creation of this plan.

5.0 Phase III - Security in the Implementation Phase

To ensure information security is addressed in the Implementation Phase, Divisions and Offices shall implement and integrate all information system security controls in the production environment. Upon completion of security control implementation and integration, an assigned workforce member(s) must perform an information system certification and accreditation review. The information system certification and accreditation will allow the information system and its security controls to be simulated in a test environment. Testing the information system and security controls will ensure the integrity and functionality of the information system.

Divisions and Offices shall not use production ("live") data during system testing unless there are no other alternatives. In those cases where the use of production data is necessary for testing, the Division or Office management must approve the use of the data, and all appropriate security controls need to be in place, just as if the data were still in production.

Results from the certification and accreditation review must be recorded, secured, and safeguarded. For assistance in completing the Security Certification and Accreditation process, please see the NC DHHS Security Standards, Administrative Security Standards – Information Security Certification and Accreditation Standard.

6.0 Phase IV - Security in the Operations and Maintenance Phase

Information systems in the production environment are subject to information technology changes throughout their lifecycle. To ensure proper information security is addressed in the Operations and Maintenance Phase, the Divisions and Offices must establish a change management process that complies with the NC DHHS Security Standards, Administrative Security Standards – Information Security Change Management Standard. This will ensure that changes to information systems are assessed, implemented, documented, secured, and safeguarded.

An assigned workforce member must continually monitor information system security controls to ensure that the security controls are effective throughout the Operations and Maintenance Phase. This will require workforce members to conduct proper periodic security control testing and evaluation. Divisions and Offices must determine when workforce member(s) will conduct testing and evaluation.

Divisions and Offices must also determine how workforce members will continuously monitor security controls.

7.0 Phase V - Security in the Disposition Phase

Disposing of information systems must be done only after a formal decision has been made by the Division or Office. Divisions and Offices must ensure that proper steps are taken to protect the security of the information developed by the information system. Divisions and Offices must adhere to the NC DHHS Security Standards, Physical Security Standards – Asset Inventory and Control Standard to ensure that security is incorporated into the Disposition Phase. Incorporating security into the disposition phase will ensure the following:

- Confidential data and/or information is properly removed from storage media
- Hardware and software is disposed of appropriately

8.0 Information System Documentation

Whether an information system is developed by Division or Office workforce members or by a third-party vendor, the information system must include proper documentation. Proper documentation consists of the Divisions and Offices creating, maintaining, securing, and safeguarding system documentation libraries. The documentation libraries will store security information regarding the five SDLC phases. Please see the following documentation guidelines:

Guidelines:

Division and Office management must consider, but not limit consideration to, the following information security documentation issues:

- A lack of documentation may have the following effects:
  - Greatly increase the risk of a serious information security incident
  - Compromise performance of routine system maintenance, especially as the complexity of the information system increases
- The information system documentation must be a required component of the system's inventory of assets (along with the physical and software assets that constitute the system)
- The information system documentation should be protected from unauthorized access by keeping it secured and safeguarded and by utilizing an access list limited to the management approved workforce members

A copy of information system documentation should be maintained for disaster recovery and business continuity, and must be stored off site.

References:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 4 – Purchasing and Maintaining Commercial Software, Section 01: Purchasing and Installing Software –
    - Standard 040101 – Specifying User Requirements for Software
    - Standard 040106 – Technical Vulnerability Management
  - Chapter 4 – Purchasing and Maintaining Commercial Software, Section 03: Other Software Issues
    - Standard 040301 – Disposing of Software
- NC Statewide Information Security Manual, Version No. 1
  - Chapter 8 – Developing and Maintaining In-House Software, Section 02: Software Development
    - Standard 080201 – Software Development
    - Standard 080206 – Separating System Development and Operations
  - Chapter 8 – Developing and Maintaining In-House Software, Section 03: Testing and Training
    - Standard 080301 – Controlling Test Environments
    - Standard 080302 – Using Live Data For Testing
    - Standard 080303 – Testing Software before Transferring to a Live Environment
  - Chapter 8 – Developing and Maintaining In-House, Section 04: Documentation –
    - Standard 080401 – Documenting New and Enhanced Systems
  - Chapter 8 – Developing and Maintaining In-House, Section 05: Other Software Development
    - Standard 080501 – Acquiring Vendor Developed Software

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Risk Management Standard
    - Information Security Certification and Accreditation Standard
- NC DHHS Security Standards
  - Application Security Standards
    - Information System Security Plan Standard
    - Information System Change Management Standard
- NC DHHS Security Standards
  - Physical Security Standards
    - Asset Inventory and Control